September 21, 2005

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.
1800 DIAGONAL ROAD
SUITE 370
ALEXANDRIA, VA 22314
US

Dear Sir/Madam,

Your refund request for 09811459 in the amount of $100.00 has been denied .

You had 8 new claims x $50.00 = $400.00 This is not an error

Sincerely,

ELEANOR KURTZ
Technical Center Others
703 308-9010 x177

U.S. Application No. «ApplicationNo»

500.39908X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Katsuyuki OKEYA

Serial No.:   09/811,459

Filed: March 20, 2001

For: METHOD OF CALCULATING MULTIPLICATION BY SCALARS
ON AN ELLIPTIC CURVE AND APPARATUS USING SAME
AND RECORDING MEDIUM

Group: 2134

Examiner: J. Lipman

Customer No.:   24956

Director of the U.S. Patent and Trademark Office
Mail Stop 16
P.O. Box 1450
Alexandria, VA 22313-1450

REQUEST FOR REFUND

Sir:

Applicants request a refund in the above-identified application due to an error

on the part of the Patent Office.

On March 1, 2005, Applicants filed an Amendment containing claims in

excess of twenty (20). A total of fourteen (14) claims had been previously filed, of

which eight (8) were independent claims. The March 1, 2005 amendment added

eight (8) claims, all of which were dependent claims.

However, the Applicants' representatives Monthly Statement of Account for

March, 2005 (copy enclosed) indicates that on March 11, 2005, Applicants were

charged $200.00 for two independent claims. A copy of the claims from the

Appl. No. 09/811,459   500.39908X00
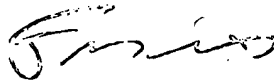Request for Refund dated July 6, 2005

amendment filed on March 1, 2005 is enclosed as evidence that the additional

claims were dependent claims and the charge for additional claims should have

been $100.00

    Please credit a refund in the amount of $100.00 to the Deposit Account No.

50-1417.

<div align="center">

Respectfully submitted,

MATTINGLY, STANGER & MALUR, P.C.

_____
Frederick D. Bailey
Registration No. 42,282

</div>

FDB/kkt
(703) 684-1120

United States Patent and Trademark Office

JUL 0 6 2005

Deposit Account Statement

Requested Statement Month:	March 2005
Deposit Account Number:	501417
Name:	MATTINGLY STANGER & MALUR, P .C.
Attention:	
Address:	1800 DIAGONAL ROAD, SUITE 370
City:	ALEXANDRIA
State:	VA
Zip:	22314
Country:	UNITED STATES OF AMERICA

DATE	SEQ	POSTING REF TXT	ATTORNEY DOCKET NBR	FEE CODE	AMT	BAL
03/03	1	09518690	ASA-761-03	1806	$180.00	$9,511.00
03/03	2	09518675	ASA-761-02	1806	$180.00	$9,331.00
03/03	207	5644539	566.104760	8008	$200.00	$9,131.00
03/03	208	09103056	566.104760	8008	$200.00	$8,931.00
03/07	2	09645450	ASA-912	1203	$300.00	$8,631.00
03/07	147	11070885	WL-103	1081	$120.00	$8,511.00
03/08	1	10694771	H-593-04	1806	$180.00	$8,331.00
03/09	99	11072414	T&A-138	1081	$240.00	$8,091.00
03/11	1	09811459	500.39908X00	1202	$400.00	$7,691.00
03/11	7	5644539		8009	$440.00	$7,251.00
03/14	33	11052787	ASA-715-06	1081	$500.00	$6,751.00
03/15	20	11057495	H-772-06	1081	$500.00	$6,251.00
03/16	2	09923427	500-40449X00	1201	$200.00	$6,051.00
03/16	3	09923427	500-40449X00	1202	$50.00	$6,001.00
03/16	280	PCT/US05/07624	WRR-105-PCT	1702	$633.00	$5,368.00
03/16	282	PCT/US05/07624	WRR-105-PCT	1703	$117.00	$5,251.00
03/16	283	PCT/US05/07624	WRR-105-PCT	8007	$40.00	$5,211.00
03/17	30	11057755	500.43322CX02	1201	$200.00	$5,011.00
03/18	32	10418360	520.38682CX1	1464	$130.00	$4,881.00
03/18	33	10418360	520.38682CX1	1801	$790.00	$4,091.00
03/21	18	11059651	NIT-458	1081	$250.00	$3,841.00
03/31	301	10828283	NIT-316-02	1501	$1,400.00	$2,441.00
03/31	301	09884067	500.40255X00	1251	$120.00	$2,321.00
03/31	302	10828283	NIT-316-02	1504	$300.00	$2,021.00

START BALANCE	SUM OF CHARGES	SUM OF REPLENISH	END BALANCE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Katsuyuki OKEYA

Serial No.:   09/811,459

Filed: March 20, 2001

For: METHOD OF CALCULATING MULTIPLICATION BY SCALARS ON AN ELLIPTIC CURVE AND APPARATUS USING SAME AND RECORDING MEDIUM

Group: 2134

Examiner: J. Lipman

AMENDMENT

Commissioner for Patents   March 1, 2005
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Office Action dated October 1, 2004, the period for reply thereto being extended two months by the attached Petition for Extension of Time to expire March 1, 2005, reconsideration and withdrawal of the outstanding rejections and allowance of the present application are respectfully requested in view of the following amendments and remarks.

Amendments to the Claims begin on page 2.

Remarks are included following the amendments.

Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the

application:

Listing of Claims:

1. (currently amended) A scalar multiplication calculation method in an elliptic

curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar

value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising

the steps of:

judging determining a value of a bit of said scalar value; and

executing operations on said elliptic curve a predetermined number of times

and in a predetermined order without depending on said judged determined value of

said bit to calculate a scalar multiplied point;

wherein said operations include calculations of addition and doubling, said

operations being selected for scalar values of one or zero, the scalar value

determining the selection of said addition and doubling calculations executed.

2. (currently amended) A scalar multiplication calculation method in an elliptic

curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar

value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising

the steps of:

judging determining a value of a bit of said scalar value; and

executing calculations of addition on said elliptic curve and doubling on said

elliptic curve in the order that said doubling on said elliptic curve is executed after

said addition on said elliptic curve is executed to calculate a scalar multiplied point;

2

wherein said addition and doubling calculations are selected for scalar values of one or zero, the scalar value determining the selection of said addition and doubling calculations executed.

3. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising

doubling calculations executed.

5. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

executing addition on said elliptic curve;

judging determining a value of a bit of said scalar value; and

executing doubling calculations on said elliptic curve to calculate a scalar multiplied point;

wherein said doubling calculations are selected for scalar values of one or zero, the scalar value determining the selection of said doubling calculations executed.

6. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve;

judging determining a value of a bit of said scalar value; and

executing said addition on said elliptic curve and said doubling on said elliptic curve in said order randomized by said step of randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve to calculate a scalar multiplied point;

4

wherein said calculations of addition and doubling are selected for scalar values of one or zero, the scalar value determining the selection of said addition and doubling calculations executed.

7. (currently amended) A scalar multiplication calculation method in an elliptic curve cryptosystem for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising the steps of:

judging determining a value of a bit of said scalar value;

randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve; and

executing said addition on said elliptic curve and said doubling on said elliptic curve in said order randomized by said step of randomizing calculation order of addition on said elliptic curve and doubling on said elliptic curve to calculate a scalar multiplied point;

wherein said calculations of addition and doubling are selected for scalar values of one or zero, the scalar value determining the selection of said addition and doubling calculations executed.

8. (original) A data generation method for generating second data from first data, comprising the step of calculating a scalar multiplication by use of a scalar multiplication calculation method according to any one of Claims 1 to 7.

9. (original) A signature generation method for generating signature data from data, comprising the step of calculating a scalar multiplication by use of a scalar

multiplication calculation method according to any one of Claims 1 to 7.

10. (original) A decryption method for generating decrypted data from encrypted data, comprising the step of calculating a scalar multiplication by use of a scalar multiplication calculation method according to any one of Claims 1 to 7.

11. (currently amended) A scalar multiplication calculator for calculating a scalar multiplied point on the basis of a scalar value and a point on an elliptic curve in an elliptic curve cryptosystem, comprising:

bit value ~~judgement~~ judgment means for ~~judging~~ determining a value of a bit of said scalar value;

addition operation means for executing addition calculations on said elliptic curve; and

doubling operation means for executing doubling calculations on said elliptic curve;

wherein after the value of said bit of scalar value is ~~judged~~ determined by said bit value ~~judgement~~ judgment means, said addition on said elliptic curve and said doubling on said elliptic curve are executed by said addition operation means and said doubling operation means a predetermined number of times and in a predetermined order so as to calculate a scalar multiplied point,

wherein said addition and doubling calculations are selected for scalar values of one or zero, the scalar value determining the selection of said addition and doubling calculations executed.

12. (original) A recording medium for storing a program relating to a scalar

6

multiplication calculation method according to any one of Claims 1 to 7.

13. (original) A scalar multiplication calculation method according to any one of Claims 1 to 7, wherein a Montgomery-form elliptic curve is used as said elliptic curve.

14. (original) A scalar multiplication calculation method according to any one of Claims 1 to 7, wherein an elliptic curve defined on a finite field of characteristic 2 is used as said elliptic curve.

15. (new) The multiplication calculation method according to claim 1, wherein

calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the double point of the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

17. (new) The multiplication calculation method according to claim 3, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the double point of the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

18. (new) The multiplication calculation method according to claim 4, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

doubling calculations include doubling the double point of the point (m+1)P to obtain

2((m+1)P) where m comprises the scalar value and P comprises the point.

21. (new) The multiplication calculation method according to claim 7, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the double point of the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.

22. (new) The multiplication calculation method according to claim 11, wherein when the value of the bit of the scalar value is 0, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the point mP to obtain 2(mP) where m comprises the scalar value and P comprises the point, and

wherein when the value of the bit of the scalar value is 1, the addition calculation includes adding a point mP to a double point of the point (m+1)P and the doubling calculations include doubling the double point of the point (m+1)P to obtain 2((m+1)P) where m comprises the scalar value and P comprises the point.